U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 471.XX

Approved: XX-XX-02

SUBJECT: RANDOM INSPECTION OF UNCLASSIFIED GOVERNMENT-OWNED COMPUTERS

1. OBJECTIVES. To establish a program that strengthens the Department of Energy's (DOE) ability to detect the presence of unauthorized information in unclassified DOE-owned computers as they are moved in and out of government facilities. This program is a response to the growing number of security incidents involving unclassified DOE computers when they are transported.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. DOE Elements. Except for the exclusions in paragraph 3.c, this Order applies to DOE elements, including the National Nuclear Security Administration (NNSA) as listed on Attachment 1.

   b. Contracts.

      (1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that will apply to contractors responsible for the management and operation of the Department-owned facilities (hereafter referred to as site/facility management contractors) whose contracts include the CRD.

      (2) This CRD must be included in all site/facilities management contracts that contain the clause at 48 CFR 952.204-2, Security requirements.

      (3) This directive does not automatically apply to other than site/facility management contracts. Application of any requirements of this directive to other than site/facility management contracts will be communicated separately from this directive. (See Section 5. Responsibilities.)

(4) The officials identified in Section 5., Responsibilities, are responsible for notifying the contracting officers of which contracts are affected. Once notified, the contracting officer is responsible for incorporating this Order into the affected contracts to comply with Laws, Regulations, and Departmental Directives clause of the affected contracts.

(5) As the Laws, Regulations, and Departmental Directives clause of site/facility management contract states, regardless of performance of the work, the site/facility management contractors with the CRD incorporated into their contract are responsible for compliance with the requirements of the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontractors at any tier to the extent necessary to ensure compliance with these requirements.

c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, the Director of the Naval Nuclear Propulsion Program will determine the applicability of this Order for activities and facilities under his control.

4. REQUIREMENTS.

a. Implementation Plans. A phased implementation plan shall be developed by the Director, Office of Security within 90 days of the effective date of this Order. The Office of Security shall also ensure that full implementation of this Order is accomplished within 1 year of the effective date of this Order. Within 6 months of the effective date of this Order, organizations should begin incorporating the attached CRD into designated contracts. Site/facility management contractors should develop an implementation plan that details how they will track and randomly inspect 20 percent of their unclassified systems that are moved into and out of DOE facilities each year. The first year can be based on the site's best estimate. The projections for other years shall be based on actual numbers from the previous year.

b. Deviations. Deviations from the requirements in this Order must be processed in accordance with DOE O 470.1, *Safeguards and Security Program*.

c. All unclassified Government-owned laptop and/or desktop computers procured with Government funds and issued by DOE and DOE contractor facilities will be subject to a random inspection for the unauthorized presence of classified information. Such inspections will consist of the examination of all fixed and removable media assigned to a computer that is being examined for the presence of active and deleted files and fragments of the same, regardless of where they exist on the drive.

d. All Federal or contractor employees who use unclassified DOE-owned laptop and/or desktop computers that were procured with Government originated funds and are issued by and removed from the facilities are required to sign the following consent form before use:

CONSENT TO CONDITIONS AND TERMS OF USE

This is a Federal computer system and is the property of the United States Government. It is for authorized official use only. **Users (authorized or unauthorized) have no explicit or implicit expectations of privacy.**

Any or all uses of this system and all data contained on this system may be monitored, recorded, copied, audited, inspected, and disclosed to Department of Energy, law enforcement personnel, and other, authorized officials. **By using this system, the user consents to such monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties.**

Description of Item(s) *(DOE Number, Serial Number, Model Number, and any other identifying information)*:_____
_____

I am aware of and consent to the terms and conditions of use.

Print Name *(First, MI, Last)*:_____
Signature:_____ Date:_____

e. Each element within DOE and DOE contractor facilities allowing unclassified computers that are DOE-owned and/or procured with DOE funds to be used outside of a DOE facility must ensure that as a minimum, 20 percent of these systems are inspected each year.

f. Each element must develop a systematic process to ensure a completely random selection of identified equipment for inspection. Each element will maintain an inventory of accountable equipment, regardless of location. Inspection teams will be properly cleared, and they will also include authorized classifiers/declassifiers.

All computers that are used to process unclassified information and are declared excess must be inspected prior to wiping, sanitizing, and disposing of the computer system. The computer systems designated as excess are not to be included as part of the 20 percent random inspection requirement.

g. Inspections must adhere to the instructions for conducting computer inspections as set forth in Attachment 3 of this Order.

h. If classified information is discovered during an inspection, the incident will be regarded as a potential compromise and handled in accordance with Attachment 3 of this Order.

i. If evidence of other unauthorized activities (e.g., fraud, waste, or abuse) is discovered, the Office of the Inspector General must be notified.

j. Each contractor, who is using DOE-owned unclassified computers, must develop a plan to implement the above requirements and establish responsibilities for the development, implementation, and maintenance of the inspection process. The Office of Security will develop technical guidance to provide direction regarding the technical aspects of the inspection process.

k. All requirements contained in draft DOE M 473.1-1, *Physical Protection Program Manual*, apply to contractors who are responsible for operating and/or administering the DOE's and the National Nuclear Security Administration's (NNSA) physical protection program and/or for protecting Security interests. The requirements in draft DOE M 473.1-1 must be assigned to all subcontractors who have responsibilities for operating, administering, and/or protecting DOE Security interests.

l. Definitions. Terms commonly used in the program are defined in the Safeguards and Security Glossary of Terms.

5. RESPONSIBILITIES.

a. Director, Office of Security.

(1) Develops guidance regarding the technical aspects of the random inspection process.

(2) Manages the Computer Forensic Laboratory.

(3) Coordinates procedural changes with the Cyber Security Policy Working Group.

b. Cyber Forensics Laboratory.

(1) Provides training on the forensics tools and software.

(2) Provides forensics tools and software to organizations listed in Attachment 1.

c. Heads of Field Elements.

(1) Review procurement requests for new non-site/facility management contracts, and if appropriate, ensure that the clause at 48 CFR 952.204-2, Security requirements, and the requirements of the CRD of this directive are included in the contract.

(2) Develop and submit implementation plans as required.

d. Heads of Headquarters Departmental Elements and the Power Marketing Administrations. Review procurement requests for new non-site/facility management contracts, and, if appropriate ensure that the clause at 48 CFR 952.204-2, Security require ments, and the requirements of the CRD of this directive are included in the contract.

e. Lead Program Secretarial Officers.

(1) Ensure that facilities under their cognizance have implemented this Order.

(2) Notify contracting officers of affected site/facility management contracts to incorporate the CRD of this directive into those contracts. Ensure procurement requests for new non-site/facility management contracts require inclusion in the resulting contracts, if appropriate, of the clause at 48 CFR 952.204-2, Security Requirements and this CRD.

f. Contracting Officers.

(1) After notification by the appropriate program official, incorporate the CRD into the affected site/facility management contracts in accordance with the Laws, Regulations, and Department of Energy Acquisition Regulations Directives clause of the contracts.

(2) Assist originators of procurement requests who want to incorporate the clause at 48 CFR 952.204-2, Security requirements, and the requirements of the CRD of this directive in new non-site/facility management contracts, as appropriate.

6. CONTACT. Questions concerning this Order should be directed to the Cyber Forensics Laboratory Program Manager, Office of Security, at (301) 903-5284.

BY ORDER OF THE SECRETARY OF ENERGY:

DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH
DOE O 471.XX, *Random Inspection of Unclassified Government - Owned Computers,*
IS APPLICABLE

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Security
Office of Worker and Community Transition
Office of Energy Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE O 471.XX, *Random Inspection of Unclassified Government-Owned Computers*

1. Purpose. This Contractor Requirements Document (CRD) is issued to aid procurement request initiators in identifying requirements that must be incorporated into contracts by contracting officers. The following requirements are based on statutes, Executive Orders, and National Directives that are designed to deter unauthorized access to classified and unclassified controlled information.

2. Applicability. The requirements listed in paragraph 5 apply to the Department of Energy (DOE) prime contractors. Regardless of who performs the work, the contractor is responsible for compliance with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with these requirements.

3. Contractors must also adhere to applicable DOE cyber security directives provided by either the Under Secretary for Energy, Science and Environment; the Administrator, NNSA; the Director, Office of Security; or the DOE Chief Information Officer (CIO) as appropriate.

   a. Contractors must protect cyber information and electronic information systems commensurate with the risk they face, and the magnitude of harm that could result from the loss, misuse, disclosure, or unauthorized modification of information processed, stored, or transmitted.

   b. Contractors must ensure cyber security competencies within their workforce so that all personnel are able to and responsible for protecting information within their span of control.

   c. Contractors must amend their DOE Cyber Security Management Program (CSMP) at all levels by meeting the requirements established in O 471.XX, *Random Inspections on Unclassified Government-Owned Computers.*

   d. Contractors must meet PSO Cyber Security Plan (PCSP) requirements when such plans cover DOE cyber assets under the contractor's ownership or control.

   e. Contractors must develop and/or implement and/or maintain separate Cyber Security Program Plans (CSPP's) for cyber assets when required by the DOE CIO.

   f. Contractors must comply with the requirements of, and achieve the objectives of applicable laws, regulations, Executive Orders, National Directives, and DOE Directives, including DOE O 471.2A, *Information Security Program Order*, and its successors.

g. Cyber resources covered by the CSMP, including PCSP's and CSPP's, and operated by contractors, must be approved according to the DOE Certification and Accreditation process.

h. Contractors must support and fulfill the cyber security performance assessment approaches identified in DOE cyber security directives and PCSP's as appropriate.

i. Contractors must budget for and apply appropriate resources for planning, implementing and maintaining on-going random inspections.

4. REQUIREMENTS.

a. All unclassified Government-owned laptop and/or desktop computers procured with Government funds and issued by DOE and DOE contractor facilities will be subject to a random inspection for the unauthorized presence of classified information. Such inspections will consist of the examination of all fixed and removable hard disk drives assigned to a computer being examined for the presence of active and deleted files and fragments of the same, regardless of where they exist on the drive.

b. All Federal or contractor employees who use unclassified DOE-owned laptop and/or desktop computers that were procured with Government origin funds and are issued by and removed from the facilities are required to sign the following consent form before use:

CONSENT TO CONDITIONS AND TERMS OF USE

This is a Federal computer system and is the property of the United States Government. It is for authorized official use only. **Users (authorized or unauthorized) have no explicit or implicit expectations of privacy.**

Any or all uses of this system and all data contained on this system may be monitored, recorded, copied, audited, inspected, and disclosed to Department of Energy, law enforcement personnel, and other, authorized officials. **By using this system, the user consents to such monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties.**

Description of Item(s) *(DOE Number, Serial Number, Model Number, and any other identifying information)*: _____
_____

I am aware of and consent to the terms and conditions of use.

Print Name *(First, MI, Last)*: _____
Signature: _____ Date: _____

c. Each element within DOE and DOE contractor facilities allowing unclassified computers that are DOE-owned and/or procured with DOE funds to be used outside of a DOE facility must ensure that as a minimum, 20 percent of these systems are inspected each year.

d. Each element must develop a systematic process to ensure a completely random selection of identified equipment for inspection. Each element will maintain an inventory of accountable equipment, regardless of location. Inspection teams will be properly cleared, and they will also include authorized classifiers/declassifiers.

e. All computers that are used to process unclassified information and are declared excess must be inspected prior to wiping, sanitizing, and disposing of the computer system. The computer systems designated as excess are not to be included as part of the 20 percent random inspection requirement

f. Inspections must adhere to the instructions for conducting computer inspections as set forth in Attachment 3 of this Order.

g. If classified information is discovered during an inspection, the incident will be regarded as a potential compromise and handled in accordance with Attachment 3 of this Order.

h. If evidence of other unauthorized activities (e.g., fraud, waste, or abuse) is discovered, the Office of the Inspector General must be notified.

i. Each contractor, who is using DOE-owned unclassified computers, must develop a plan to implement the above requirements and establish responsibilities for the development, implementation, and maintenance of the inspection process. The Office of Security will develop technical guidance to provide direction regarding the technical aspects of the inspection process.

j. All requirements contained in draft DOE M 473.1-1, *Physical Protection Program Manual*, apply to contractors who are responsible for operating and/or administering the DOE's and the National Nuclear Security Administration's physical protection program and/or for protecting security interests. The requirements in draft DOE M 473.1-1 must be assigned to all subcontractors who have responsibilities for operating, administering, and/or protecting DOE security interests.

INSTRUCTIONS FOR CONDUCTING COMPUTER INSPECTIONS

DOE O 471.XX, *Random Inspection of Unclassified DOE-Owned Computers*

1. INTRODUCTION. These instructions are to be followed during the conduct of computer inspections. Since not all of the instructions are appropriate in every situation, implement only those procedures, which are appropriate for a given situation. Inspections will be conducted whether or not the equipment is marked with DOE property tags.

2. REFERENCE. Technical guidance is available for use by personnel conducting the inspections. This is a controlled document, available from the Office of Security at (301) 903-5284.

3. COMPUTER ON-SITE INSPECTION PROCEDURES.

   a. Computer Selection.

      (1) All computers that processed unclassified information and declared as excess must be inspected prior to wiping, sanitizing, and disposing of the hard drive using the tools and software from the Cyber Forensics Laboratory.

      (2) DOE elements must implement a computer selection process to ensure that the appropriate percentage of computers, based on paragraph 4 of the Order, are inspected annually. Return each computer to the list of inspection candidates after inspection. The selection process will ensure the following:

         (a) That no activity is operationally burdened by the unavailability of a high percentage of computers being inspected;

         (b) That users of computers to be inspected are notified immediately and directed to deliver their computers within 24 hours of notification. The facility/complex director may authorize no-notice pickups of computers for inspection. Exceptions to the delivery requirements could be granted if the individual is on travel or if the inspection will cause unacceptable delays to work deadlines. The cognizant DOE authority must justify and validate all exceptions in writing.

         (c) That the selection process is completely random without regard to department, organization, or individual.

   b. Conduct of Inspection. The trained designated personnel on site will conduct an initial text string examination. The appropriate text string search software will be designated and validated by the DOE Cyber Forensics Lab to ensure no unintentional or accidental "writes" will occur to the computer system(s) being inspected. If the text string search does not reveal any classified information residing on the inspected computer system, it will be returned to the user.

c. Procedure in the Event Classified or Other Unauthorized Activity is Discovered. In the event evidence of unauthorized activity or classified information is suspected to reside on the computer system, during any phase of the examination, it is imperative the guidelines in subparagraphs (1) through (3) be followed. No attempt to sanitize or otherwise clean or alter the subject hard drive will be made.

(1) If any data is found indicating possible unauthorized activity (fraud, waste, and abuse), all work related to the examination will stop, the Office of the Inspector General notified, and the original computer hard drive secured.

(2) If during the examination of the system, classified data is discovered or suspected, the data will be reviewed by appropriate personnel to determine its classification. If the material is determined to be classified, all work related to the examination will stop, a security incident report will be made, and the original hard drive of the subject computer will be immediately secured in accordance with the highest classification of the information contained on the drive. The DOE Cyber Forensics Lab will then be contacted for further instructions.

(3) Examination Reporting. The log that is completed during the inspection process will suffice as the inspection report. An annual summary of examinations conducted, examination results, and the percentage of computers examined should be forwarded to the Director of the Office of Security at the end of the calendar year.

d. Return of Examined Computers. Users will be notified when their computers are ready for pick-up immediately upon successful completion of the inspection. Computers will be returned in the same operating condition as when turned in; this will be verified with the user at pick-up.

4. DOE COMPUTER LAB PROCEDURES.

a. Hard Drive Imaging. When the computer system and its hard drive and/or assigned storage-capable devices are received by the DOE Cyber Forensics Laboratory, an exact image of the drive/devices(s) will be made to perform analysis. This process is conducted to prevent the possibility of damage or alteration of the original hard drive as a result of the analysis process.

(1) Prior to imaging, the computer specifications will be recorded. Make, model, and serial number will be noted as well as physical condition, operational status, and the operating system installed. The operational condition and operating system installed will be checked while the user is present, and the user will verify the results by initialing the appropriate space on the inspection worksheet. The computer will not be booted after the incoming acceptance check until it is returned to the user.

(2) Approved software, appropriate for the operating system of the inspected computer, will be used and will include a hard drive lock to prevent accidental access or damage to the drive being imaged.

(3) A virus scan must be performed in the event the examination will be conducted using a restored image.

b. Image Examination. Examinations are to be conducted for the sole purpose of identifying the presence of classified information on computer hard drives that are designated for unclassified use.

(1) Only trained personnel in controlled access areas will perform the examinations. Any personnel not on the access list that require access to the examination area will be signed in and out of the area.

(2) The examinations will be conducted using approved software appropriate for the operating system of the inspected computer.

(3) The examination must be targeted against an image of the subject drive, never against the actual hard drive.

(4) Each step in this process and its results will be recorded on an examination log.

5. DISPOSAL OF EXCESS COMPUTERS.

a. All computers declared excess to DOE must be inspected for the presence of classified matter, prior to disposal. If no classified matter is found during the inspection, hard drives will be wiped using a disk wipe utility, validated by the DOE Cyber Forensics Laboratory, which conforms to U.S. Government requirements for secure destruction of Government data in unclassified environments.

b. If classified or other inappropriate material is discovered, examining personnel will follow established procedures in reporting their finding(s) to designated authorities.